Group Midterm Project: Designing a Cloud Solution

For TigerMed Company Startup

Hemanth Vasireddy
Harika Banda
Keerthana Komatineni

Introduction and Overview

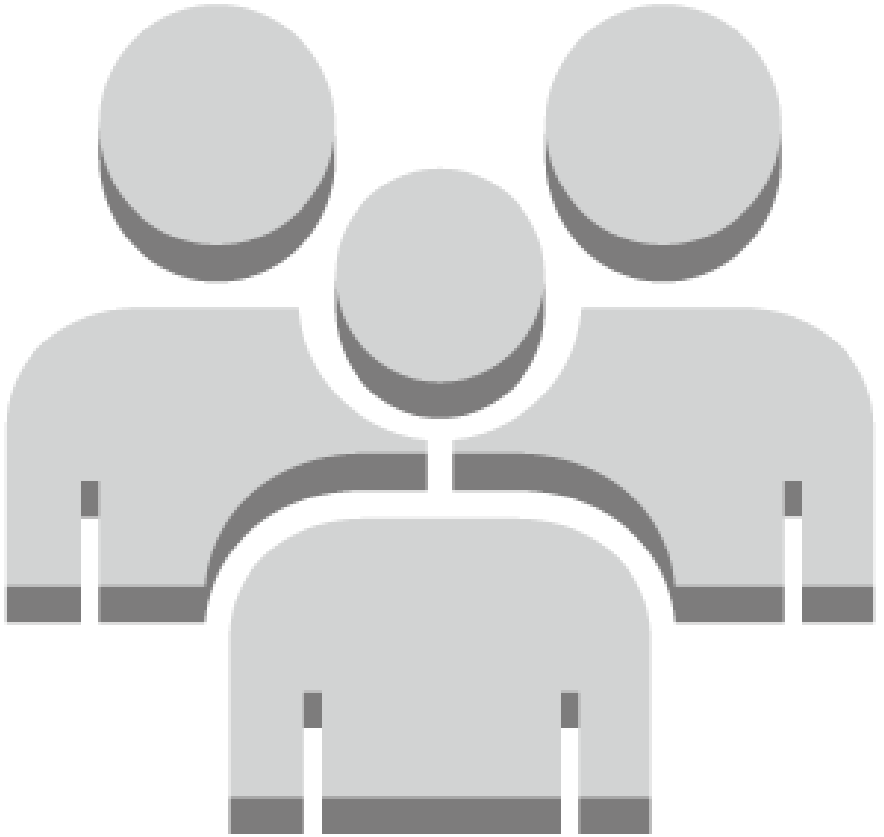
Company Background: TigerMed Company

- TigerMed Company is **a much hyped software startup company**.
- It has built **an online medical social networking and diagnosis assistance application** for users in Asia-Pacific (APAC), the US, and Europe.
- The application **connects patients and doctors to**:
  - Allow online appointments, remote consultation, remote diagnosis, electronic prescription transfer, and payment services.
  - Allow customers to upload documents and images. Text is extracted from documents, and images are converted into multiple formats.
- The application has **not yet been launched publicly**.

The Request

TigerMed Company has hired **your company** to architect a solution in AWS to meet their application needs.

In preparation for your meeting with them, they provided information about their current environment.



TigerMed Company: Current Environment

Here is some background information about TigerMed Company:

- Deployed its current development and test infrastructure **with a server hosting company**
- Uses **Microsoft Windows servers to host their web and application tiers** with **Microsoft SQL Server Standard Edition backend databases**
- The application **launch date is coming soon,** and they expect many users to start using the application
- Believes it would be best **to use cloud technologies to support its rapid growth**
- Thinks the new cloud platform could host development, test, and production environments

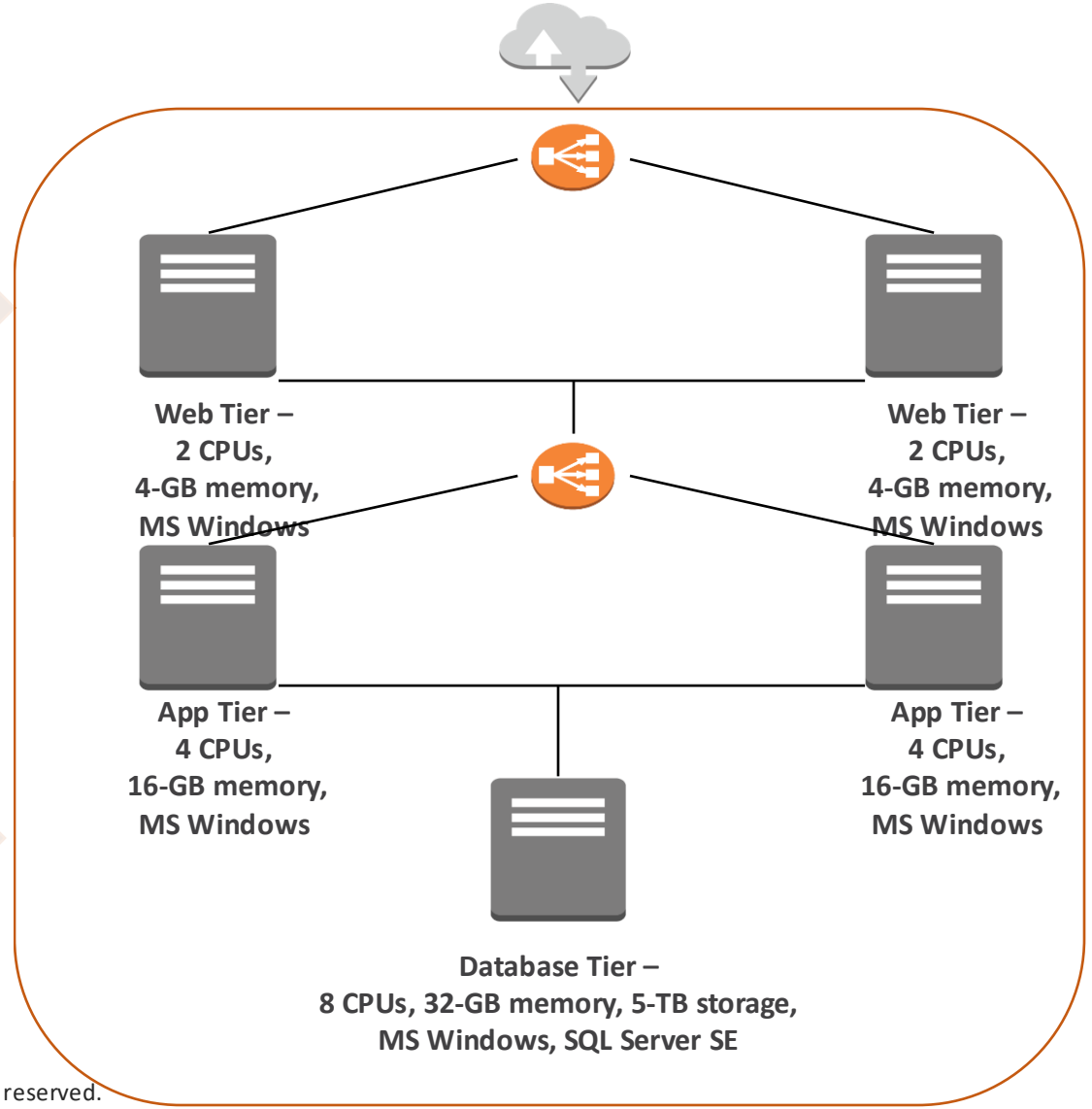
TigerMed Company: Current Environment

Web Tier:

- Two physical servers (Two CPUs / 4-GB memory)
- Microsoft Windows 2016 Base with Internet Information Services (IIS)
- High Availability load balancer used to balance traffic between the web servers

Database Tier:

- One physical server (Eight CPUs / 32-GB memory / 5-TB storage)
- SQL Server Standard Edition with Microsoft Windows 2016 Base
- DBAs access and manage the database, but no RDMBS or advanced configuration is required.



Application Tier:

- Two physical servers (Four CPUs / 16-GB memory)
- Microsoft Windows 2016 Base with Internet Information Services (IIS)
- High Availability load balancer used to balance traffic between app servers

Customer Requirements and Solution Design Worksheets

TigerMed Company Requirements

The requirements include:

1. **Configuring** access permissions to conform with AWS best practices
2. **Building** networks that conform to AWS best practices while providing all the necessary network services to the application in their different environments
3. **Building** an architecture that matches the current architecture at the server hosting company and that can handle doubling the number of servers
4. **Securing** all medical information, as medical information usually contains highly sensitive personally identifiable information (PII)
5. **Utilizing** load balancers for web tier and application tier that must support **HTTP, HTTPS, TCP protocols plans to move their application into AWS**
6. **Architecture** should be resilient (built for high availability, scale, and business continuity)
7. **Configuring** auditing to track all user actions

Potential Services

Below are the **potential** services and their purpose required to move **TigerMed's** current environment to AWS:

- **EC2 Instances:** To launch web and application instances.
- **EC2 Autoscaling:** To autoscale web and application instances on demand.
- **Route 53:** Amazon Route 53 is used for domain registration and customers can access TigerMed through the registered domain name.
- **Virtual Private Cloud (VPC):** Provides an isolated section in AWS Cloud to launch AWS resources and enables network connectivity.
- **Application load balancer:** Used to control network traffic on various EC2 instances
- **AWS Lambda:** To automatically handle computing resources required by the application
- **AWS CloudTrail:** Used for auditing, tracking account activity and also for security purposes
- **AWS CloudWatch:** Used for monitoring, Dashboard creation and reporting
- **AWS IAM:** Used to provide secure access to the application for authorized users
- **AWS KMS:** Used to provide more security to the application by creating and controlling encrypt keys for sensitive data
- **Amazon Aurora:** To handle Relational Database service
- **Amazon Simple Email Service (SES):** This service is used for email communication between customers and management.
- **Amazon Textract:** Used to extract images and text from customer documents.
- **Amazon Simple Notification Service (SNS):** Used to send notifications to set of customers based on the requirement
- **API Gateway:** Used to manage APIs.
- **NAT Gateway & Internet Gateway:** To provide internet connectivity to the subnets in VPC (Virtual Private Cloud)

Requirements – Identity and Access

There are THREE groups of people that need special permissions:

- Systems Administrator Group
- Database Administrator Group
- Monitoring Group

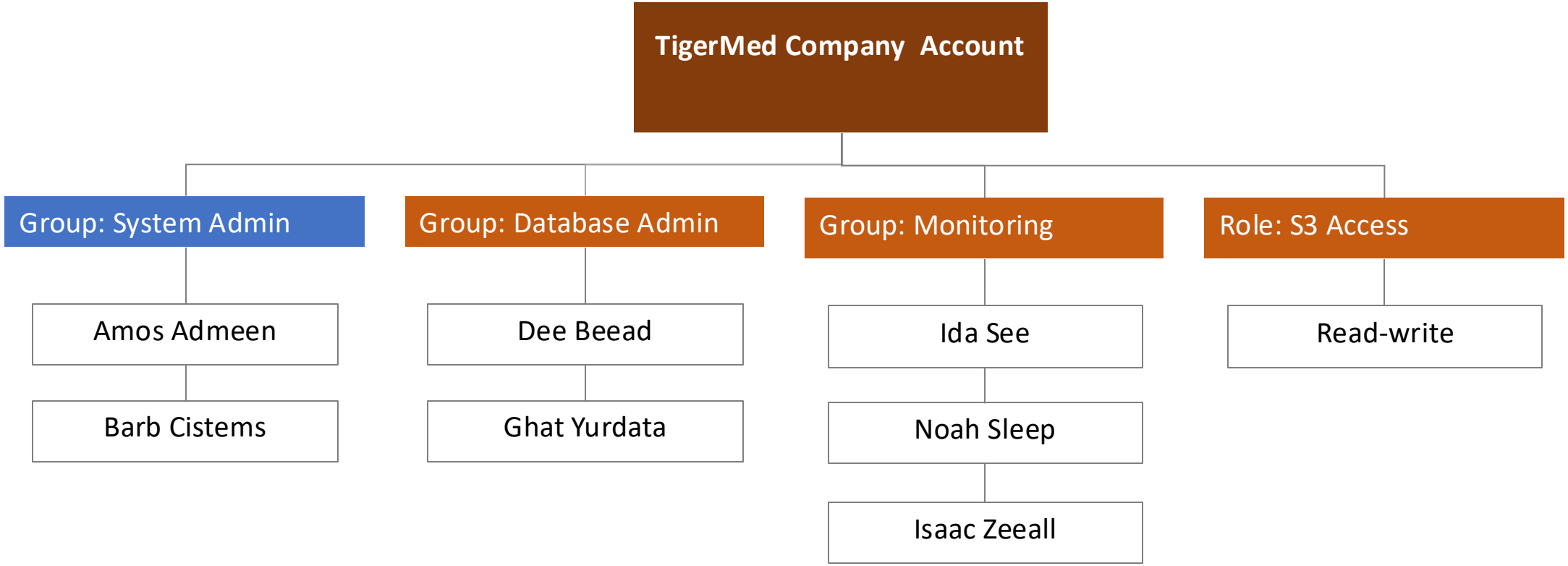
There must also be a role in place to grant permissions to the TigerMed application to read from and write to S3 buckets

These 7 people must have special permissions:

- Amos Admeen, Lead Systems Administrator
- Dee Beead, Database Administrator
- Barb Cistems, Systems Administrator
- Ida See, AWS Resource Monitor
- Noah Sleep, AWS Resource Monitor
- Ghat Yurdata, Sr. Database Administrator
- Isaac Zeeall, AWS Resource Monitor

Solution – Identity and Access Management

Use a diagram like this to document users, groups, and roles that need to be created.



Solution – Identity and Access Management

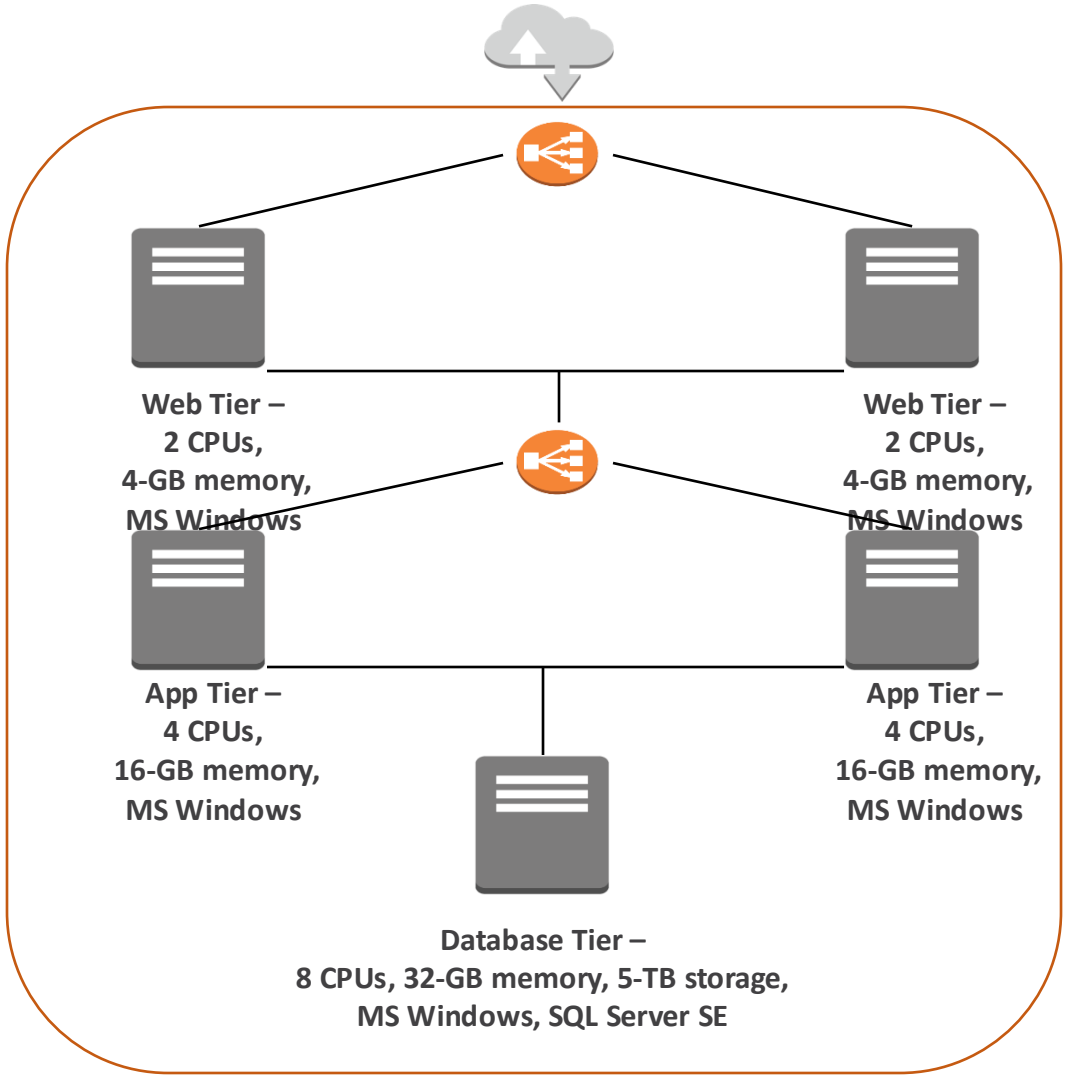
Use a table like this to work out the groups and their associated permissions.

Group/Role #	Group/Role Name	Permissions
Group	System Admin	This group has permissions to system and development operations. Then can access any AWS service except database and Monitoring solutions.
Group	Database Admin	This group has permissions to only database operations. They can also access Aurora DB.
Group	Monitoring	This group has permissions to monitoring operations. They can access AWS Cloudwatch, Cloudtrail.
Role	S3 Access	This role has read and write access to S3 buckets

Solution – User Authentication

Requirement	Solution
Passwords should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number	Using the AWS IAM password policy feature, we can enforce below password policies for IAM users. 1. Minimum password length - [8] 2. Require atleast 1 uppercase letter from Latin Alphabet (A-Z) 3. Require atleast 1 lower case letter from Latin Alphabet (a-z) 4. Require atleast 1 number 5. Require atleast 1 special (non-alphanumeric) character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ‘)
Passwords must be changed every 90 days; the last three passwords cannot be re-used	Using AWS IAM password policy, we can enforce below rules. 1. Require password expiration for every 90 days 2. Prevent reuse of last three passwords.
All administrators require programmatic access	1. IAM group of system and database administrators will be given programmatic access after creating the group. 2. IAM role of admins will be given programmatic access when needed.
Administrator sign-in to the AWS Management Console requires the use of Virtual MFA	Attach the IAM virtual MFA policy to admins as below. … "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}} …

Detailed Requirements – Architecture



Design a solution in AWS with:

1. **Networks** that conform to AWS best practices while providing all the necessary network services to the application in their different environments
2. An **architecture** that matches the current architecture at the server hosting company and that can handle doubling the number of servers
3. **Security** for all medical information, as medical information usually contains highly sensitive personally identifiable information (PII)
4. **Load balancers** for distributing traffic across resources in the web tier and app tier. Load balancers must support **HTTP and HTTP/S (and Custom TCP if used between the app tier and database tier)**

Detailed Requirements – Network and Security

The new architecture must conform to AWS best practices to:

- Achieve high availability for all tiers to reduce downtime
- Control access to the application and limit public entry points. *Note*: There should be **no external access** to the application or database tiers
- Allocate reasonably sized VPCs and network segments (subnets)
- Maintain separate networks for *TigerMed Company's* development, testing, and production environments
- Support HTTP and HTTP/S protocols (and Custom TCP protocol between the application and database tier)
- Database servers can receive requests from application servers only on port 1433 (Custom TCP)

Solution – Network Architecture

VPC	Region	Purpose	# of Subnets	# of AZs	VPC CIDR Range
1	us-east-1	Development	1 private	1(us-east-1a)	10.0.0.0/16
2	us-east-1	Testing	1 private	1(us-east-1a)	10.0.1.0/16
3	us-west-2	Deliver to US users	2 public, 3 private	2(us-west-2a, us-west-2c)	10.1.0.0/16
4	eu-west-3	Deliver to European users	2 public, 3 private	2(eu-west-3a, us-west-3b)	10.2.0.0/16
5	ap-south-1	Deliver to Asia-Pacific users	2 public, 3 private	2(ap-south-1a, ap-south-1b)	10.3.0.0/16

Solution – Network Architecture

Network Architecture for the United States Region

Subnet Name	VPC	Subnet Type (public/private)	AZ	Subnet CIDR Range
Development subnet	10.0.0.0/16	Private	us-east-1a	10.0.0.0/24
Testing subnet	10.0.0.0/16	Private	us-east-1a	10.0.1.0/24
US private subnet 1	10.1.0.0/16	Private	us-west-2a	10.1.0.0/24
US Private subnet 2	10.1.0.0/16	Private	us-west-2a	10.1.1.0/24
US public subnet 1	10.1.0.0/16	Public	us-west-2a	10.1.2.0/24
US private subnet 3	10.1.0.0/16	Private	us-west-2c	10.1.3.0/24
US private subnet 4	10.1.0.0/16	Private	us-west-2c	10.1.4.0/24
US public subnet 2	10.1.0.0/16	Public	us-west-2c	10.1.5.0/24

Solution – Network Architecture

Network Architecture for Europe and Asia-Pacific regions

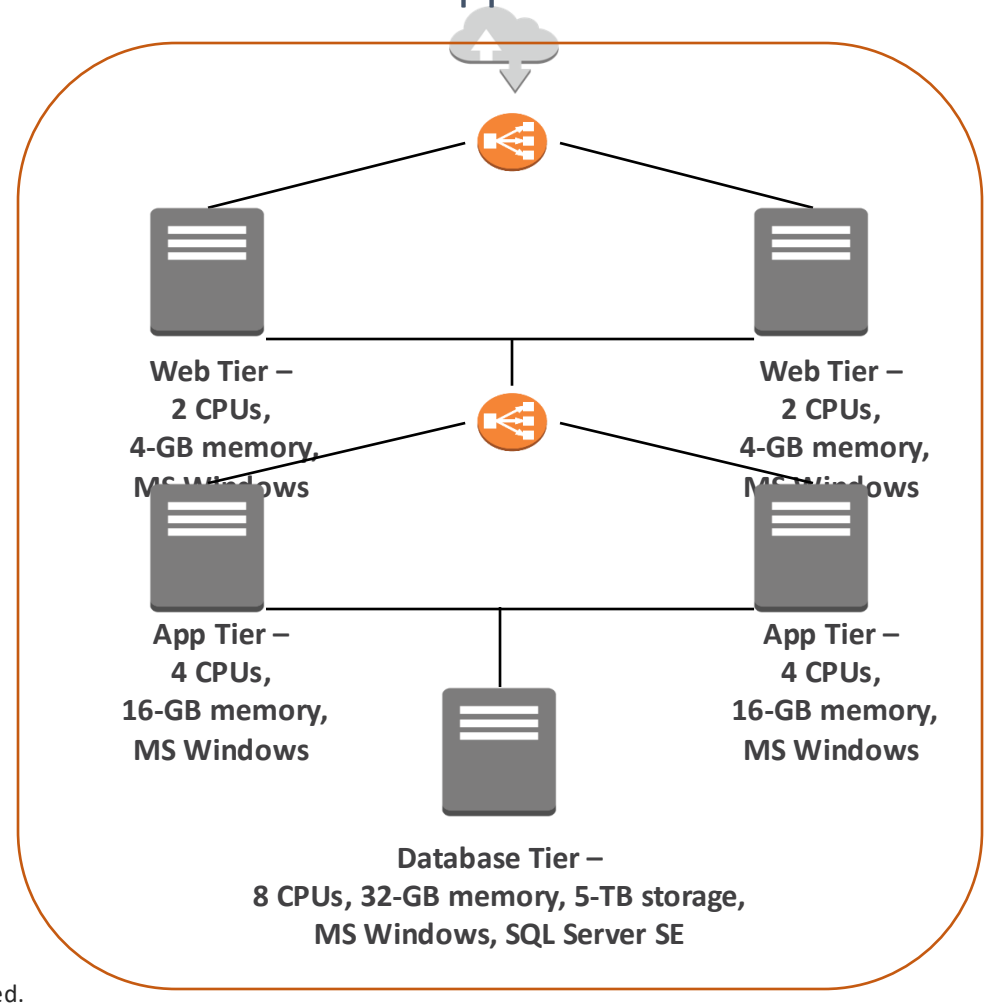
Subnet Name	VPC	Subnet Type (public/private)	AZ	Subnet CIDR Range
EU private subnet 1	10.2.0.0/16	Private	eu-west-3a	10.2.0.0/24
EU private subnet 2	10.2.0.0/16	Private	eu-west-3a	10.2.1.0/24
EU public subnet 1	10.2.0.0/16	Public	eu-west-3a	10.2.2.0/24
EU private subnet 3	10.2.0.0/16	Private	eu-west-3b	10.2.3.0/24
EU private subnet 4	10.2.0.0/16	Private	eu-west-3b	10.2.4.0/24
EU public subnet 2	10.2.0.0/16	Public	eu-west-3b	10.2.5.0/24
AP private subnet 1	10.3.0.0/16	Private	ap-south-1a	10.3.0.0/24
AP private subnet 2	10.3.0.0/16	Private	ap-south-1a	10.3.1.0/24
AP public subnet 1	10.3.0.0/16	Public	ap-south-1a	10.3.2.0/24
AP private subnet 3	10.3.0.0/16	Private	ap-south-1b	10.3.3.0/24
AP private subnet 4	10.3.0.0/16	Private	ap-south-1b	10.3.4.0/24
AP public subnet 2	10.3.0.0/16	Public	ap-south-1b	10.3.5.0/24

Solution – Web and Application Tier

Identify the type, size, and justification for the cloud instances you will use in the web and application tiers

Web Tier:

- Two physical servers (Two CPUs / 4-GB memory)
- Microsoft Windows 2016 Base with Internet Information Services (IIS)
- High Availability load balancer used to balance traffic between the web servers



Application Tier:

- Two physical servers (Four CPUs / 16-GB memory)
- Microsoft Windows 2016 Base with Internet Information Services (IIS)
- High Availability load balancer used to balance traffic between app servers

Solution – Web and Application Tier

Tier	Tags*		OS	Instance Type	Justification	# of instances	User Data? Y/N
Web	Web	Key = Name Value = Web tier	Windows	t3.large	It has 2 vCPU and 8 GB of RAM. It matches current web tier on premise specification, secure, elastic and best for general purpose computing.	2-4(2 reserved & 2 on-demand)	N
App	App	Key = Name Value = App tier	Windows	t3.xlarge	It has 4 vCPU and 16 GB of RAM. It matches current app tier on premise specification, secure, elastic and best for general purpose computing.	2-4(2 reserved & 2 on-demand)	N
DB	DB	Key = Name Value = DB tier	Windows	db.t4g.2xlarge	It has 8 vCPU and 32 GB of RAM. It supports amazon aurora, matches current db specification and most newly aws:db instance type is also supported.	1-2(1 per AZ & scalable to 2 per AZ)	Y

Solution – Security Groups

Inbound rules for our Security Groups:

Security Group	Type	Protocol	Port	Source	Description
Web	Application Load Balancer, EC2 Instance	HTTP/HTTPS	80-HTTP 443-HTTPS `	Anywhere	Allows inbound HTTP/HTTPS access from any IPv4/IPv6 address
App	Application Load Balancer, EC2 Instance	HTTP/HTTPS	80-HTTP 443-HTTPS	Web Security Group	Allows inbound HTTP/HTTPS access from any IPv4/IPv6 address
DB	Aurora	Custom TCP	3306	App Security Group	Default port to access Amazon Aurora

Detailed Requirements – High Availability

The new architecture should be designed for high availability and automatic scaling.

- The web and application tiers should be **resilient and designed for business continuity**
  - If a server becomes unavailable it will be **replaced by a new server**
  - A **server is considered unavailable** if the operating system or application fails to respond
  - New servers should come online automatically as demand increases
- The database tier should **support Multi-AZ deployment**

Detailed Requirements – High Availability

What do you need for a high-availability environment?

- We have taken ‘high availability’ criteria into consideration while designing the new AWS environment for TigerMed by making it available to users in three regions- Asia-Pacific (APAC), the US, and Europe. In a single region, we have enhanced availability by introducing multiple web and application instances, utilizing an application load balancer for effective traffic distribution. Additionally, we’ve integrated an auto-scaling group to dynamically adjust the number of EC2 instances based on workload demands. For database reliability, we've chosen Amazon Aurora, a managed AWS service that offers Availability Zone (AZ) deployment within Amazon RDS. This architectural design guarantees high availability for our web, application, and database instances, ensuring our system remains robust and responsive.

What do you need to configure automatic scaling?

- Launch Template
- Auto Scaling Group
- Scaling Policies
- CloudWatch Alarms
- Elastic Load Balancer (ELB)
- High Availability Architecture

Detailed Requirements – Auditing

Requirements

1. Continuously monitor and retain account activity related to actions across your AWS infrastructure
2. Log the event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services
3. Ensure that is an audit trail for all executed API calls
4. Ensure that logs are stored in a secure location

Auditing requirements

AWS Services used for auditing:

- **AWS CloudTrail**: AWS CloudTrail provides detailed event history of your AWS account activity, including actions taken via the AWS Management Console, AWS Command Line Interface (CLI), SDKs, and other AWS services. It helps you track changes, investigate incidents, and meet compliance requirements.

- **VPC Flow Logs**: VPC Flow Logs capture information about IP traffic flowing into and out of your VPC. These logs can be useful for monitoring and auditing network traffic.